# User-Managed Access (UMA)

http://tinyurl.com/umawg

@UMAWG

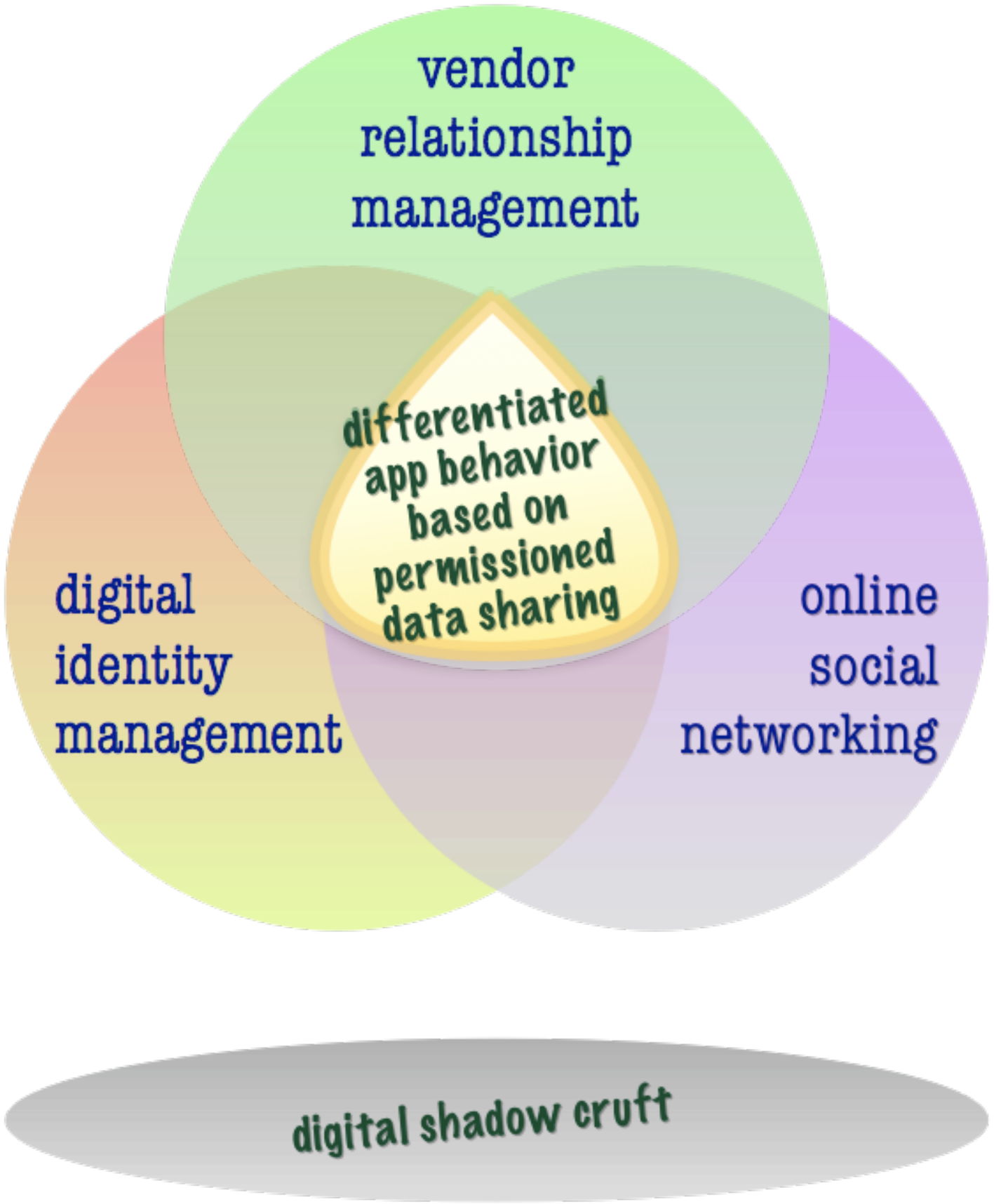
10 December 2010

kantara INITIATIVE™

# Privacy is not about secrecy

> The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be”
>
> – Ann Cavoukian, Information and Privacy Commissioner of Ontario, **Privacy in the Clouds** paper

It’s about context, control, choice, and respect

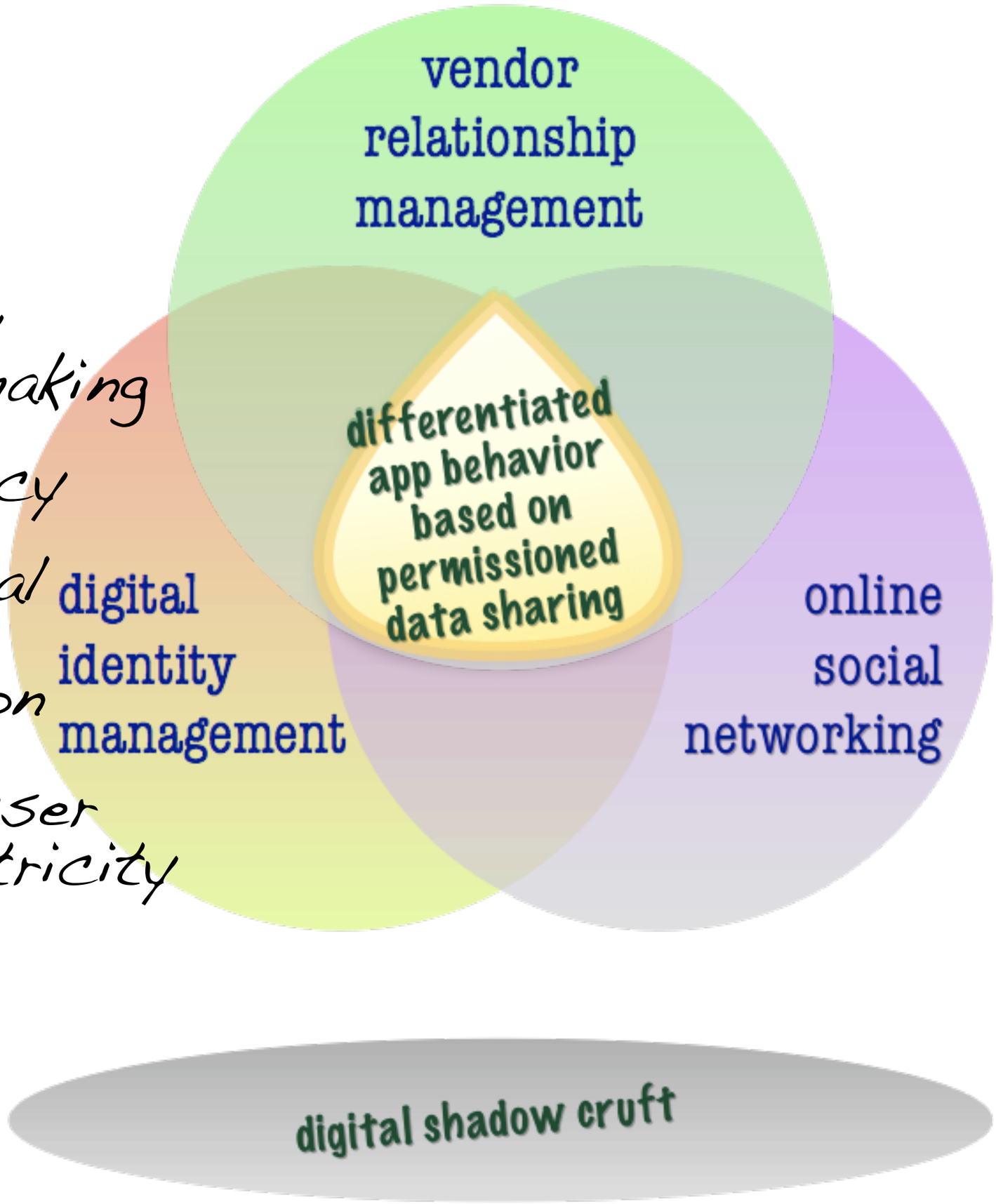

vendor
relationship
management
differentiated
app behavior
based on
permissioned
data sharing
digital
identity
management
online
social
networking
digital shadow cruft

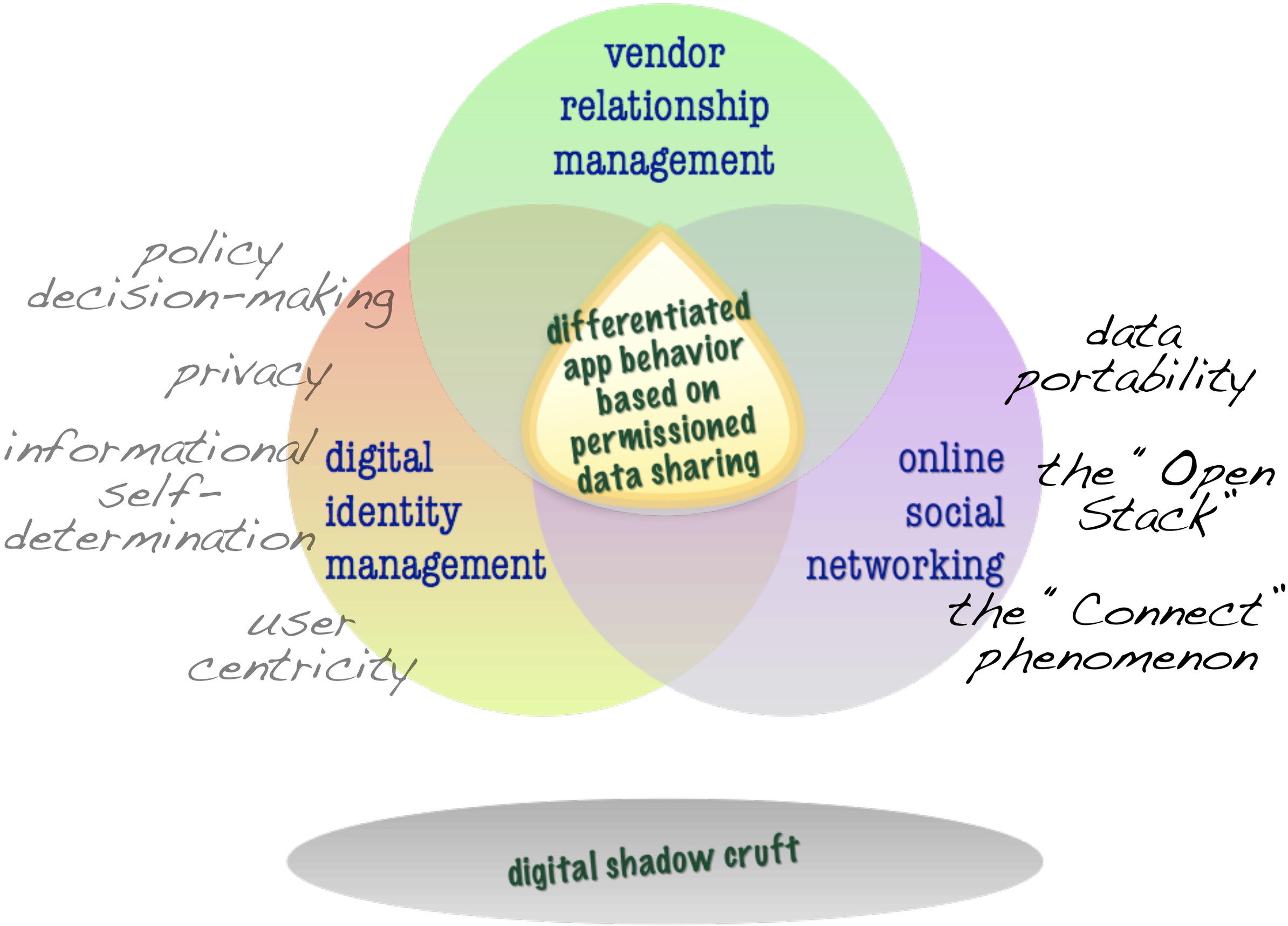
policy decision-making

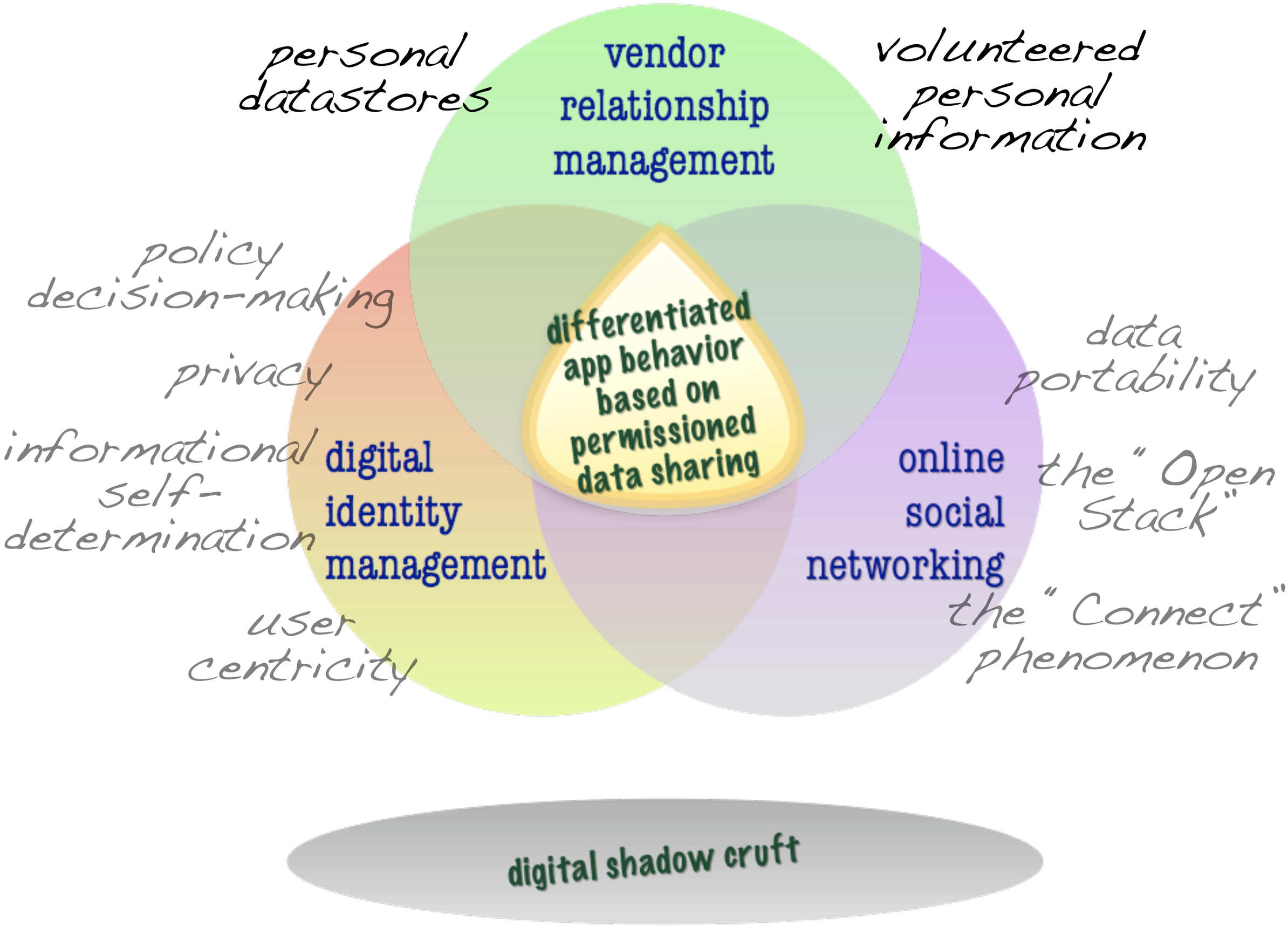
privacy

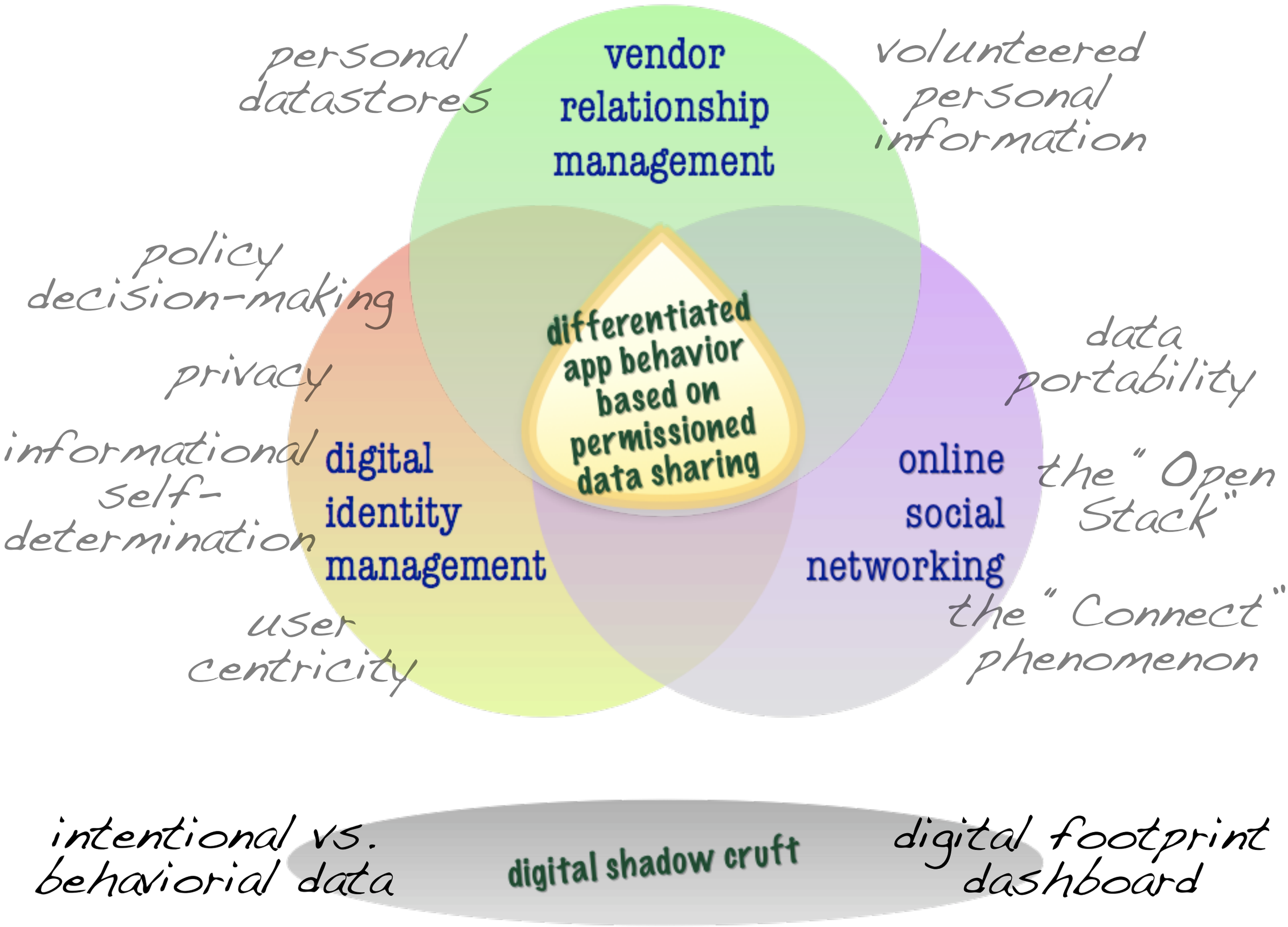
informational self-determination

user centricity




vendor relationship management
policy decision-making
privacy
informational self-determination
digital identity management
user centricity
differentiated app behavior based on permissioned data sharing
data portability
the "Open Stack"
online social networking
the "Connect" phenomenon
digital shadow cruft


personal datastores
vendor relationship management
volunteered personal information
policy decision-making
privacy
informational self-determination
digital identity management
user centricity
differentiated app behavior based on permissioned data sharing
data portability
the "Open Stack"
online social networking
the "Connect" phenomenon
digital shadow cruft


personal datastores
vendor relationship management
volunteered personal information
policy decision-making
privacy
informational self-determination
digital identity management
differentiated app behavior based on permissioned data sharing
data portability
the "Open Stack"
online social networking
the "Connect" phenomenon
user centricity
intentional vs. behavioral data
digital shadow cruft
digital footprint dashboard

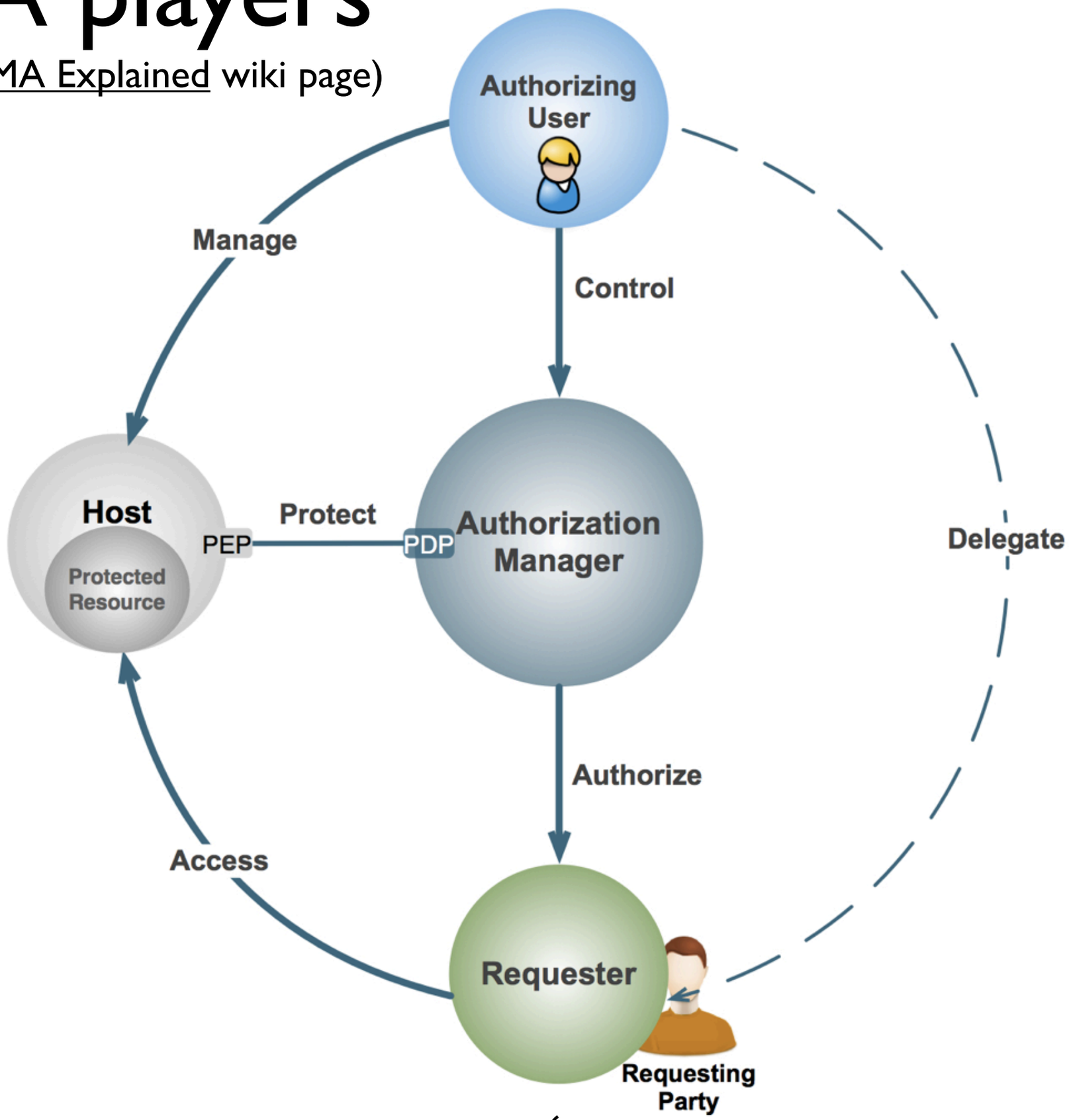
# UMA is...

- A web protocol that lets you control authorization of data sharing and service access made on your behalf
- A Work Group of the Kantara Initiative that is free for anyone to **join** and contribute to
- A set of draft specifications that is free for anyone to implement
- Undergoing multiple implementation efforts
- Slated to be contributed to the IETF
- Striving to be simple, OAuth-based, identifier-agnostic, RESTful, modular, generative, and developed rapidly

| Selective sharing shortcomings | User-Managed Access solutions |
|---|---|
| Little sophistication and consistency in Web 2.0 access control – e.g., Google Calendar vs. Flickr vs. TripIt | A way for any web app to provide sophisticated access control merely by outsourcing it, à la SSO |
| Rules for selective sharing can't be applied to different apps – the "family" ACL has to keep being rebuilt | Selective-sharing policies can be mapped to content at multiple hosts |
| Selective sharing is largely identity-based and static | Conditions for access can be "claims-based", with claims tested when access is attempted – e.g., "anyone over 18" |
| Individual is only in a position to consent to sharing and to site terms of service, not dictate terms of access | Sharing policies form a barrier; requesting parties have to agree to terms or otherwise prove suitability |
| Individual can't get a global view of every party they've said can get access to their data and content | Sharing policies and sharing authorizations all come out of a single "hub" application |
| OAuth today only enables the protection of singular API endpoints for web services | Any Web resource with a URL, and any access scope on it, can be protected – e.g., sharing a status update API or a single tweet |

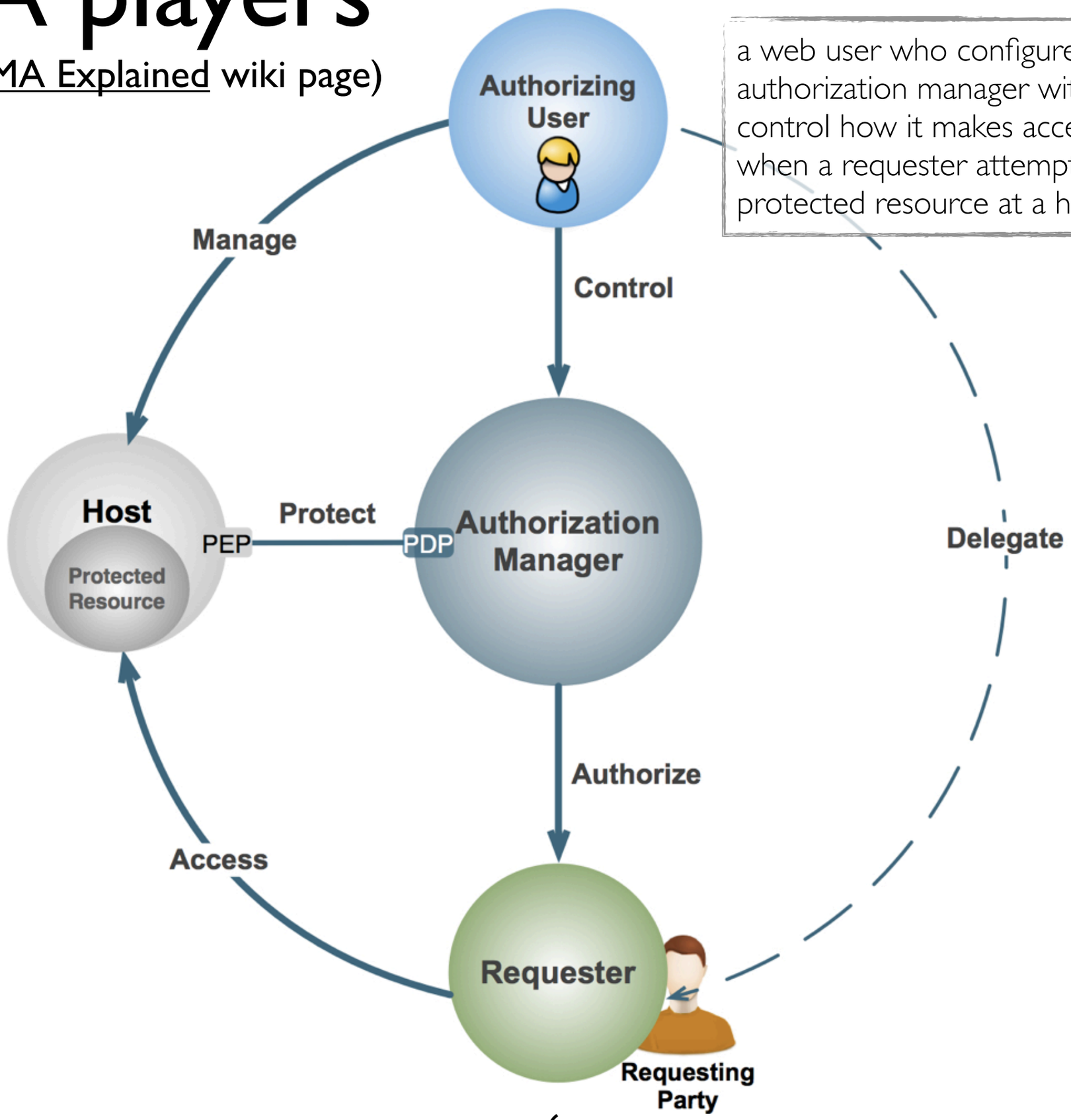
# UMA players

(see also UMA Explained wiki page)



# UMA players

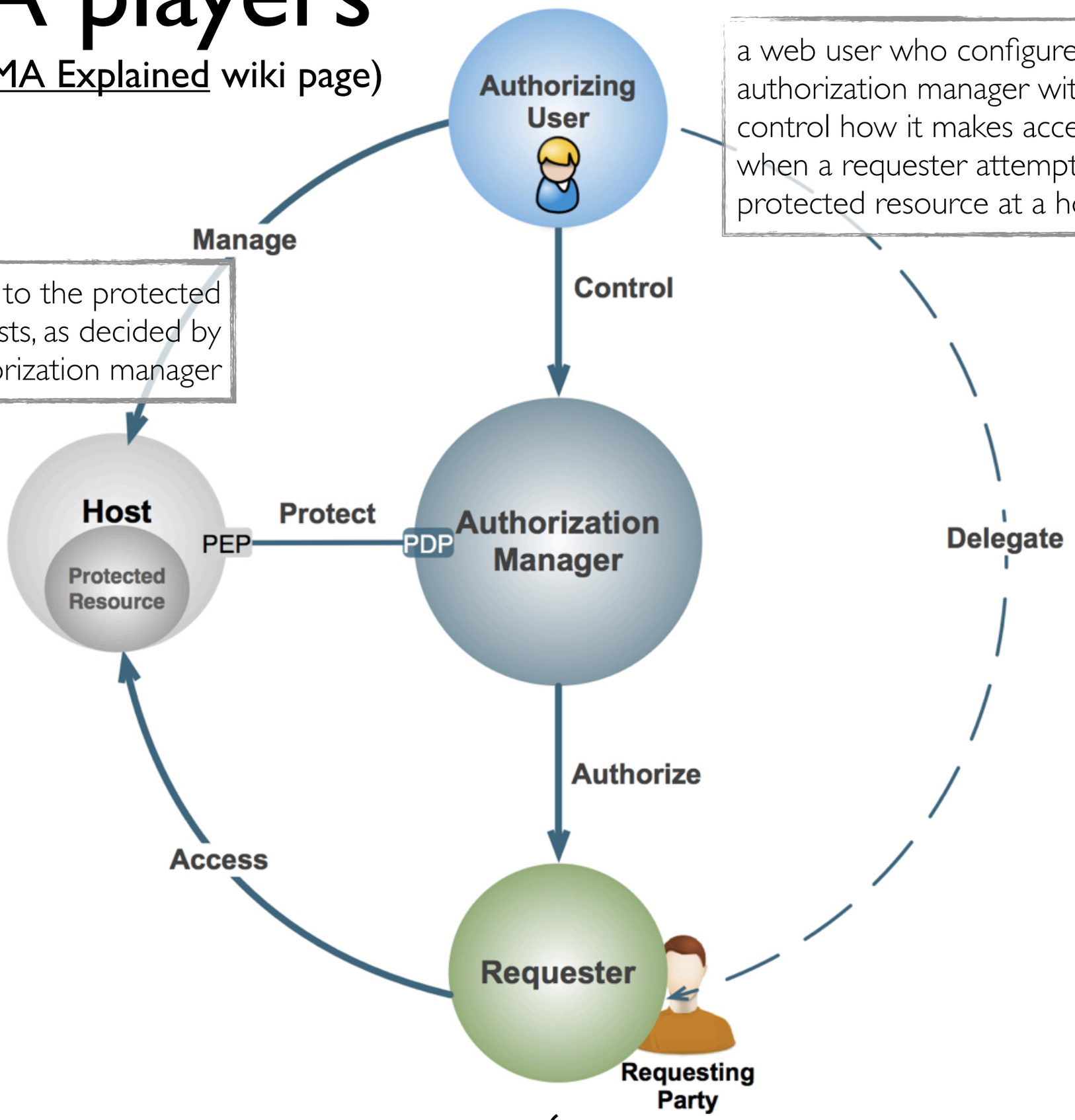
(see also UMA Explained wiki page)




a web user who configures an authorization manager with policies that control how it makes access decisions when a requester attempts to access a protected resource at a host

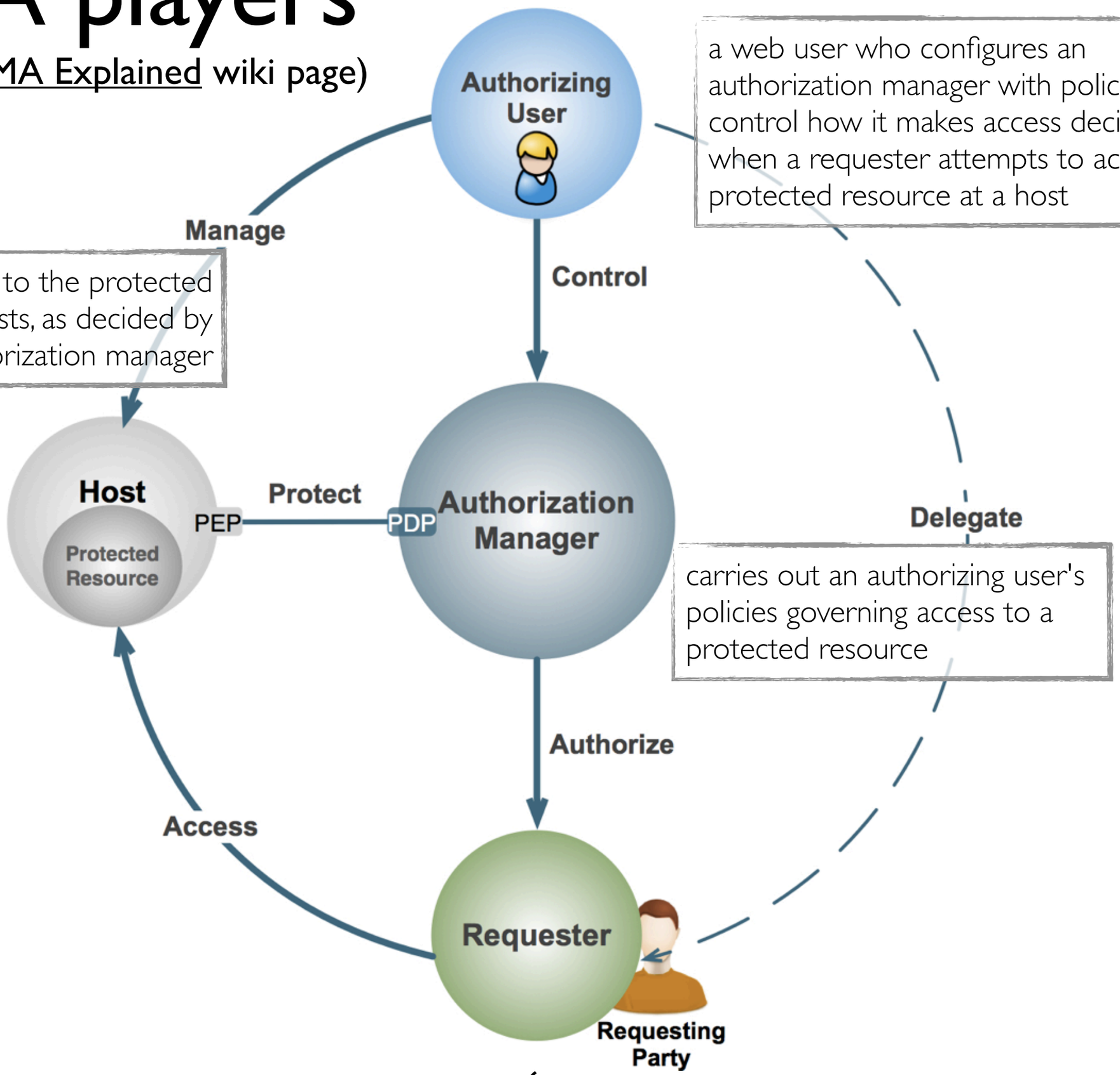
# UMA players

(see also UMA Explained wiki page)



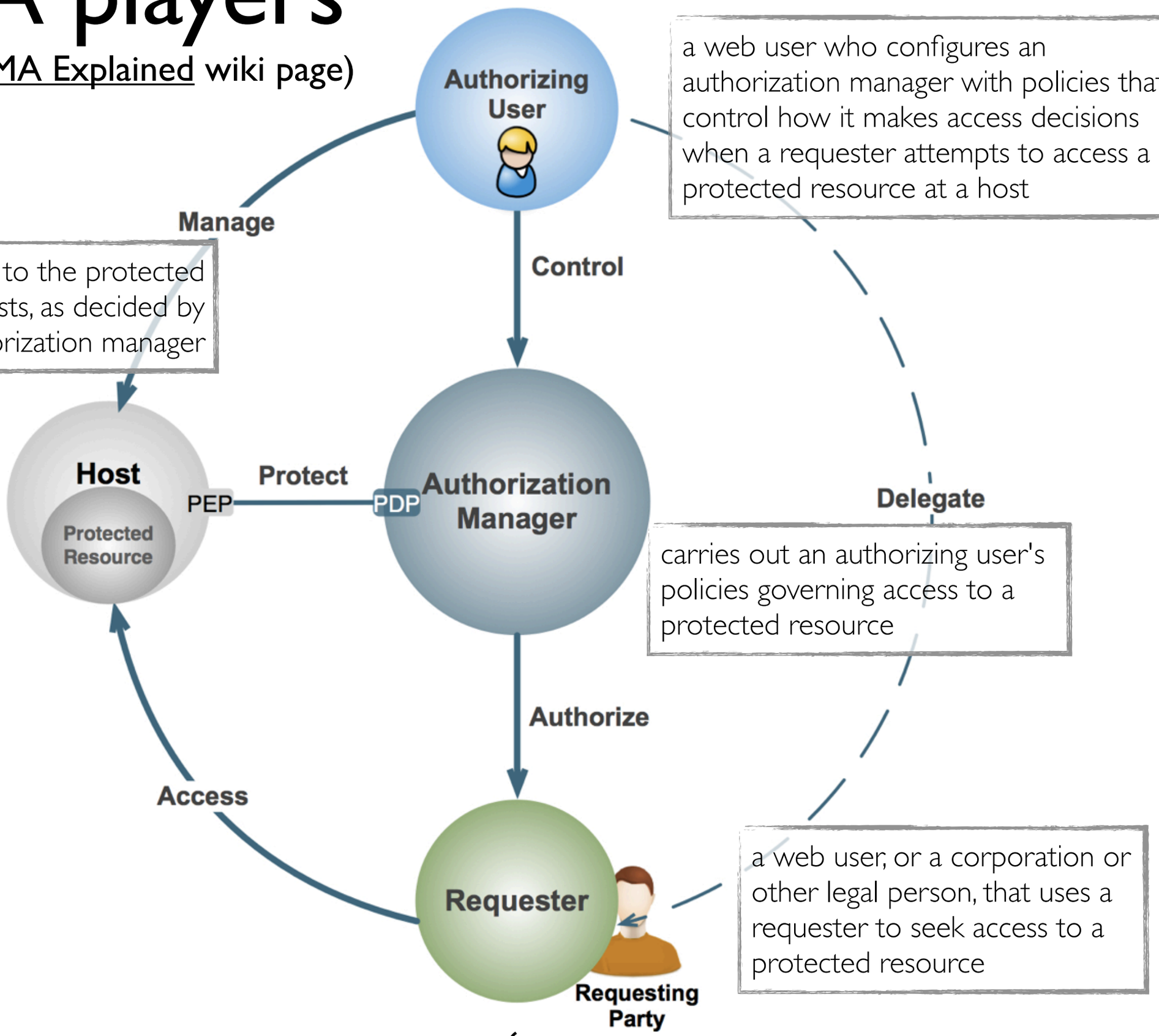
# UMA players

(see also UMA Explained wiki page)



# UMA players

(see also UMA Explained wiki page)




a web user who configures an authorization manager with policies that control how it makes access decisions when a requester attempts to access a protected resource at a host

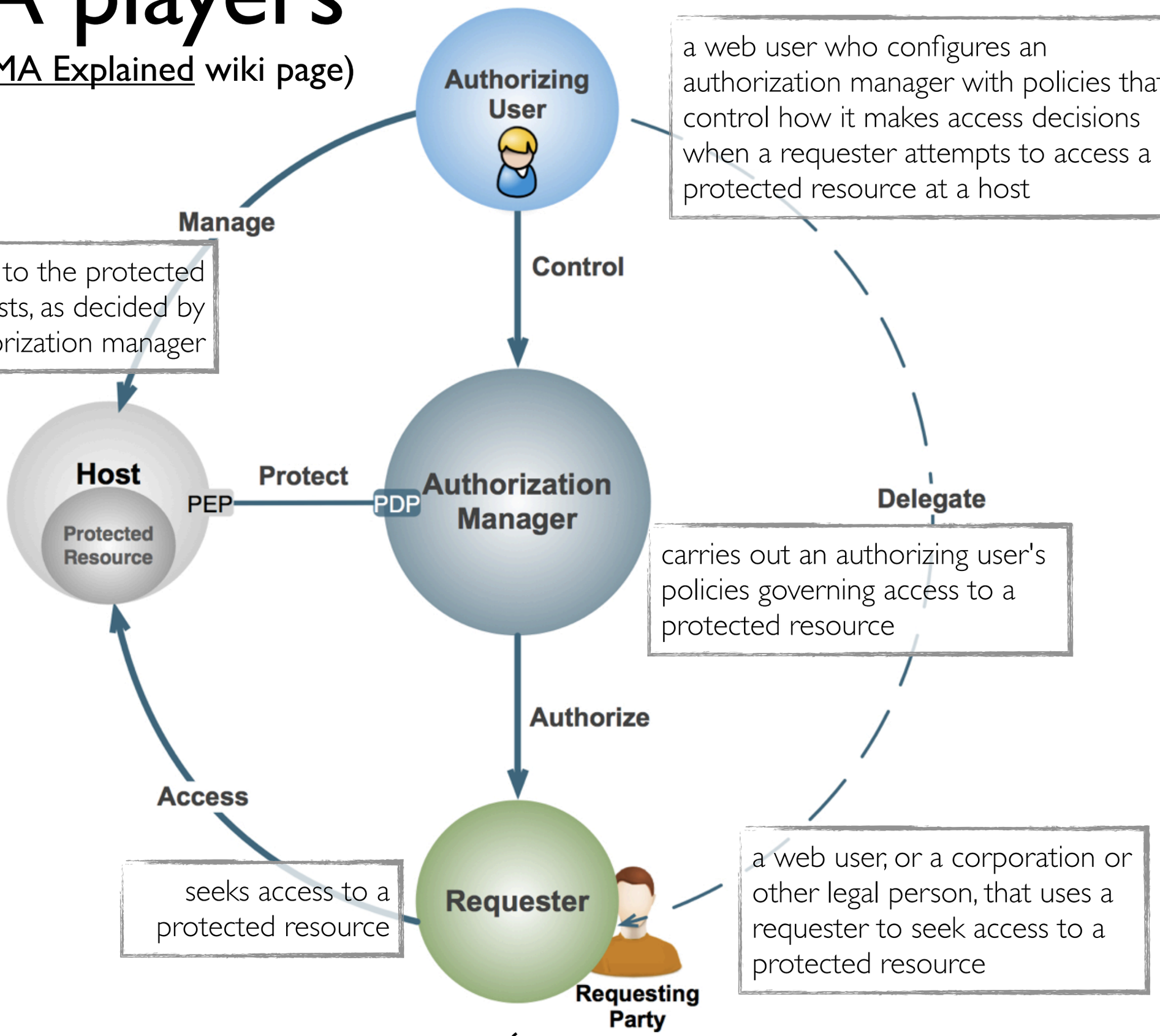
enforces access to the protected resources it hosts, as decided by an authorization manager

carries out an authorizing user's policies governing access to a protected resource

a web user, or a corporation or other legal person, that uses a requester to seek access to a protected resource

# UMA players

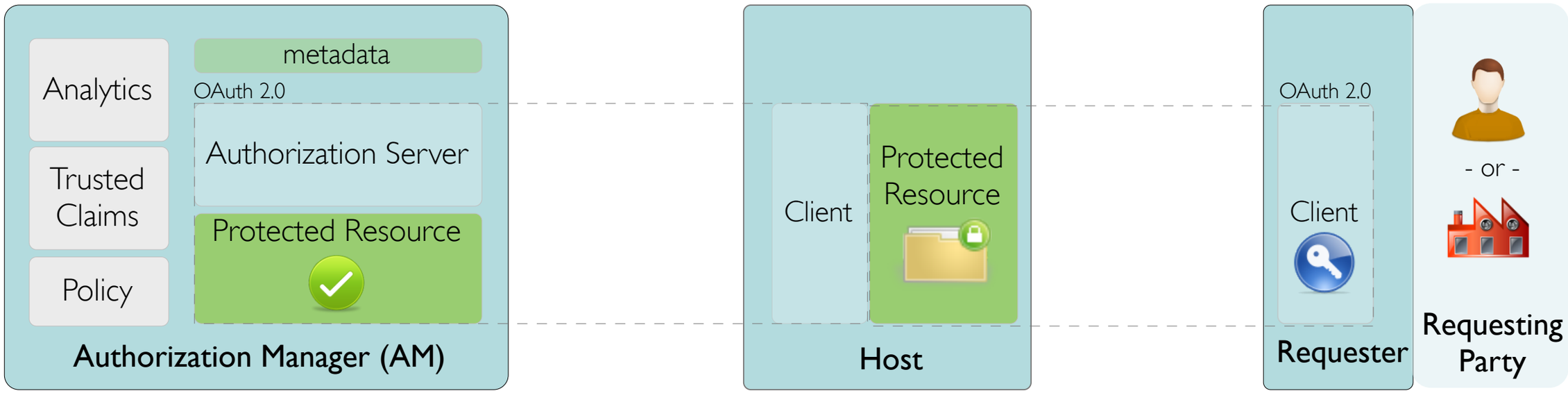
(see also UMA Explained wiki page)



# UMA has three steps

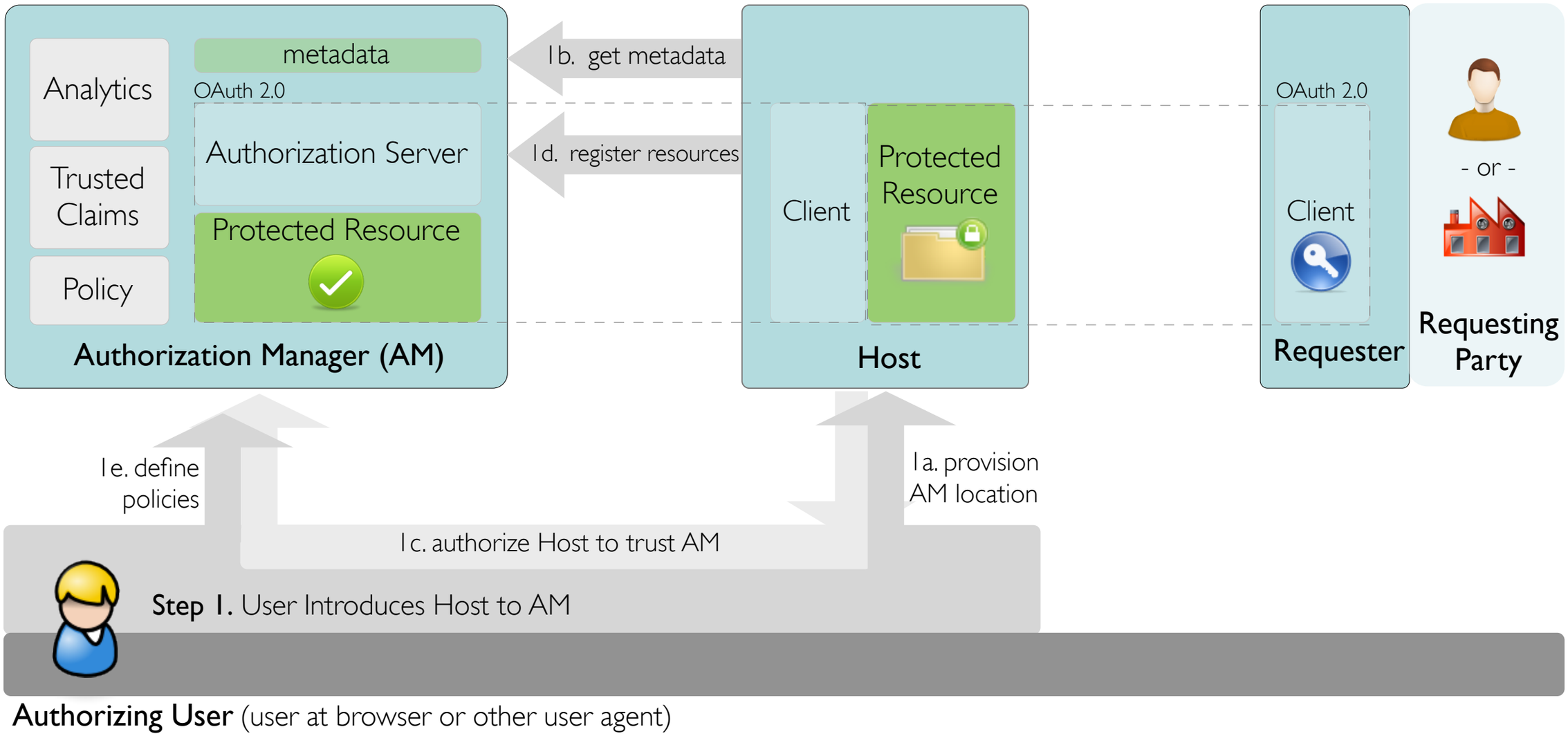
1. Trust a token
   - Alice introduces her Calendar host to CopMonkey: "When CopMonkey says whether to let someone in, do what he says"
2. Get a token
   - A travel marketing company tries to subscribe to Alice's calendar but it has to agree to her terms of use: "All right, all right, I'm clicking the 'I Agree' button"
3. Use a token
   - The marketing company now has an OAuth access token to use at the Calendar host: "This means Alice thinks it's okay"

# The players again

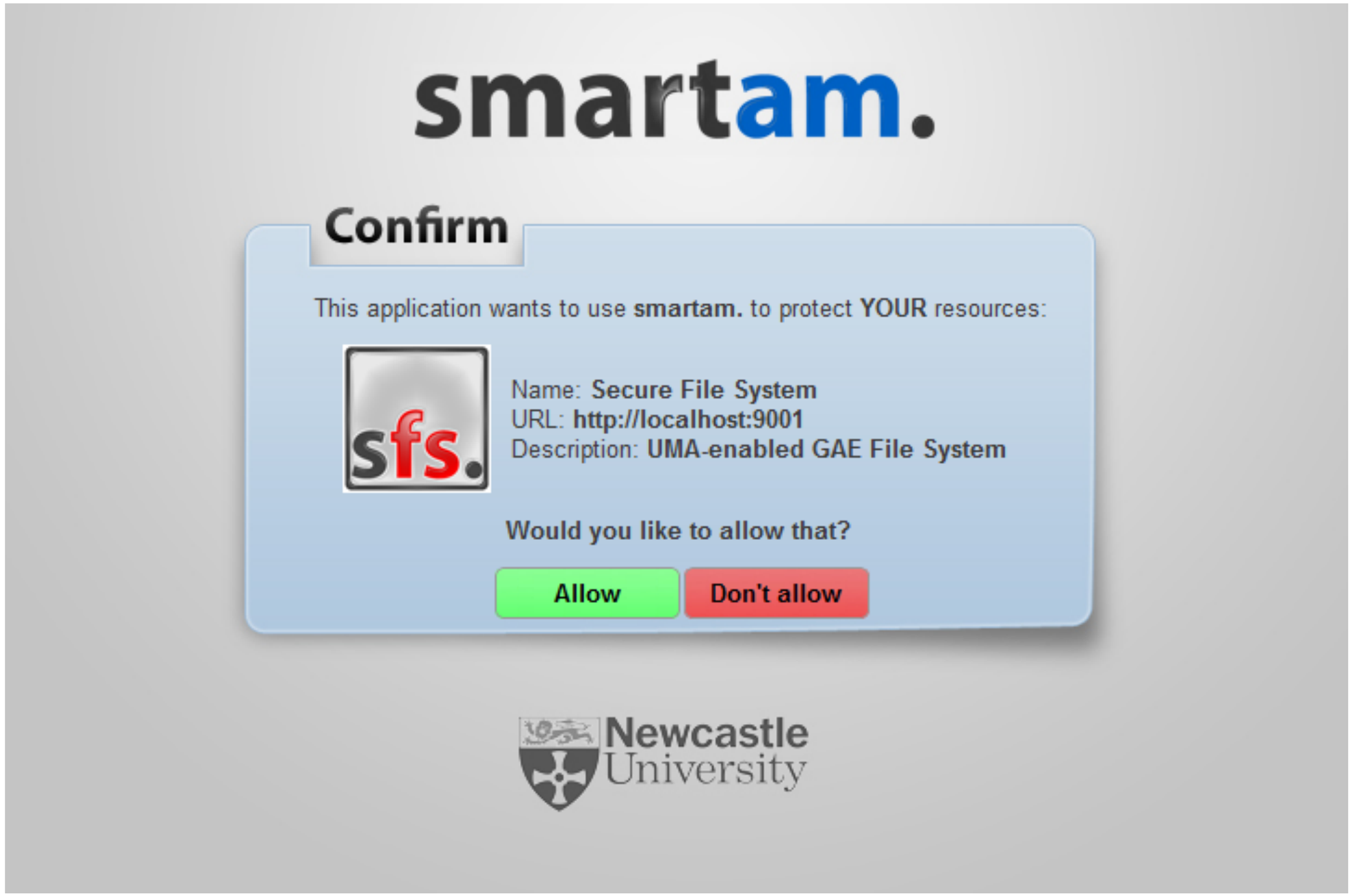


**Authorizing User** (user at browser or other user agent)

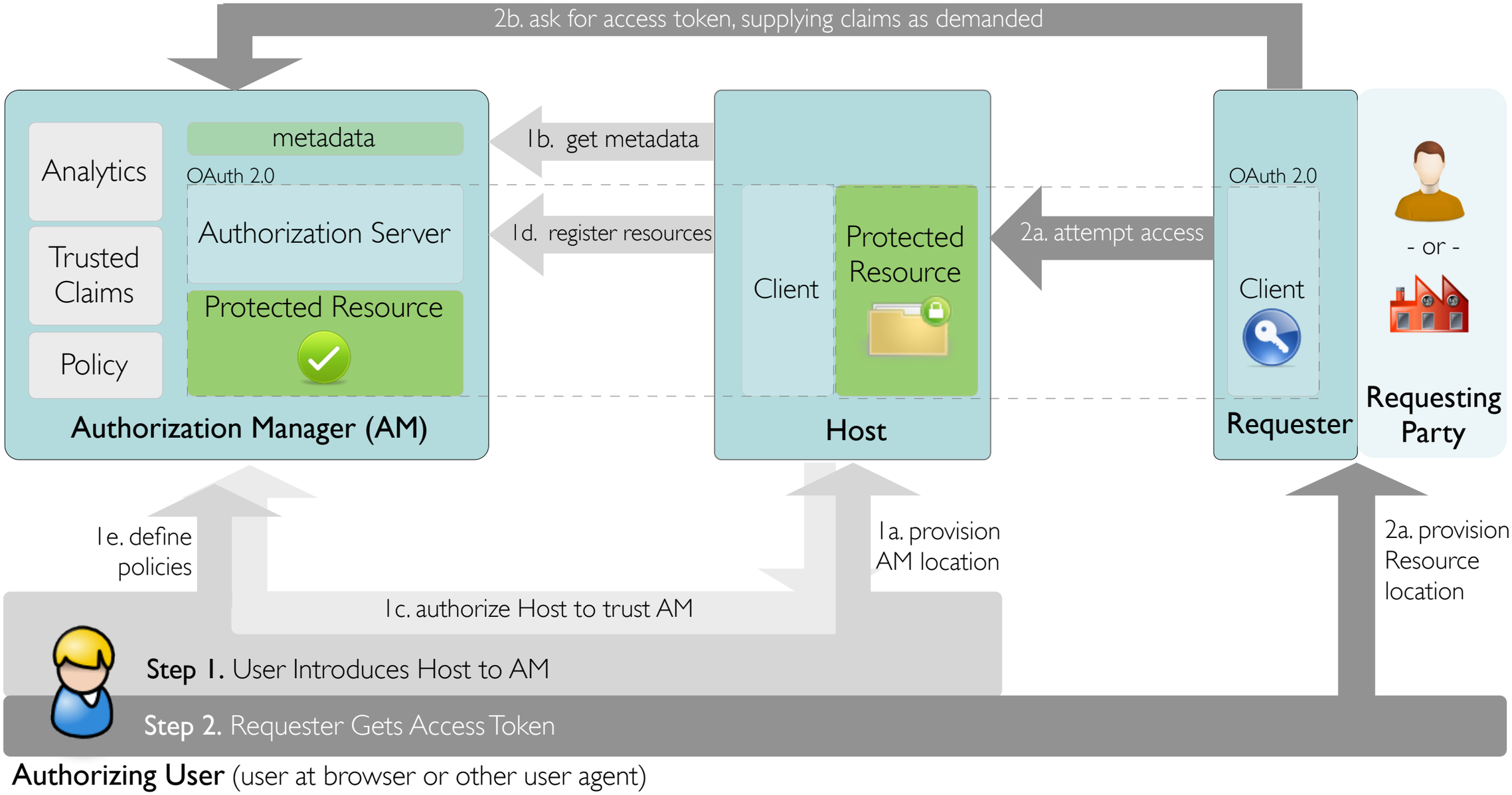
# Step 1 protocol flow



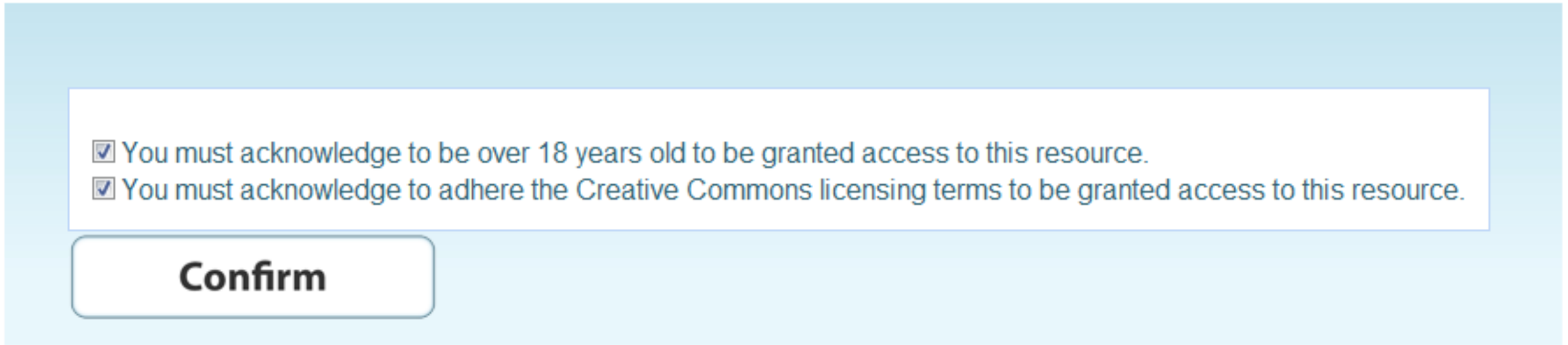
# A possible UX for host-AM introduction



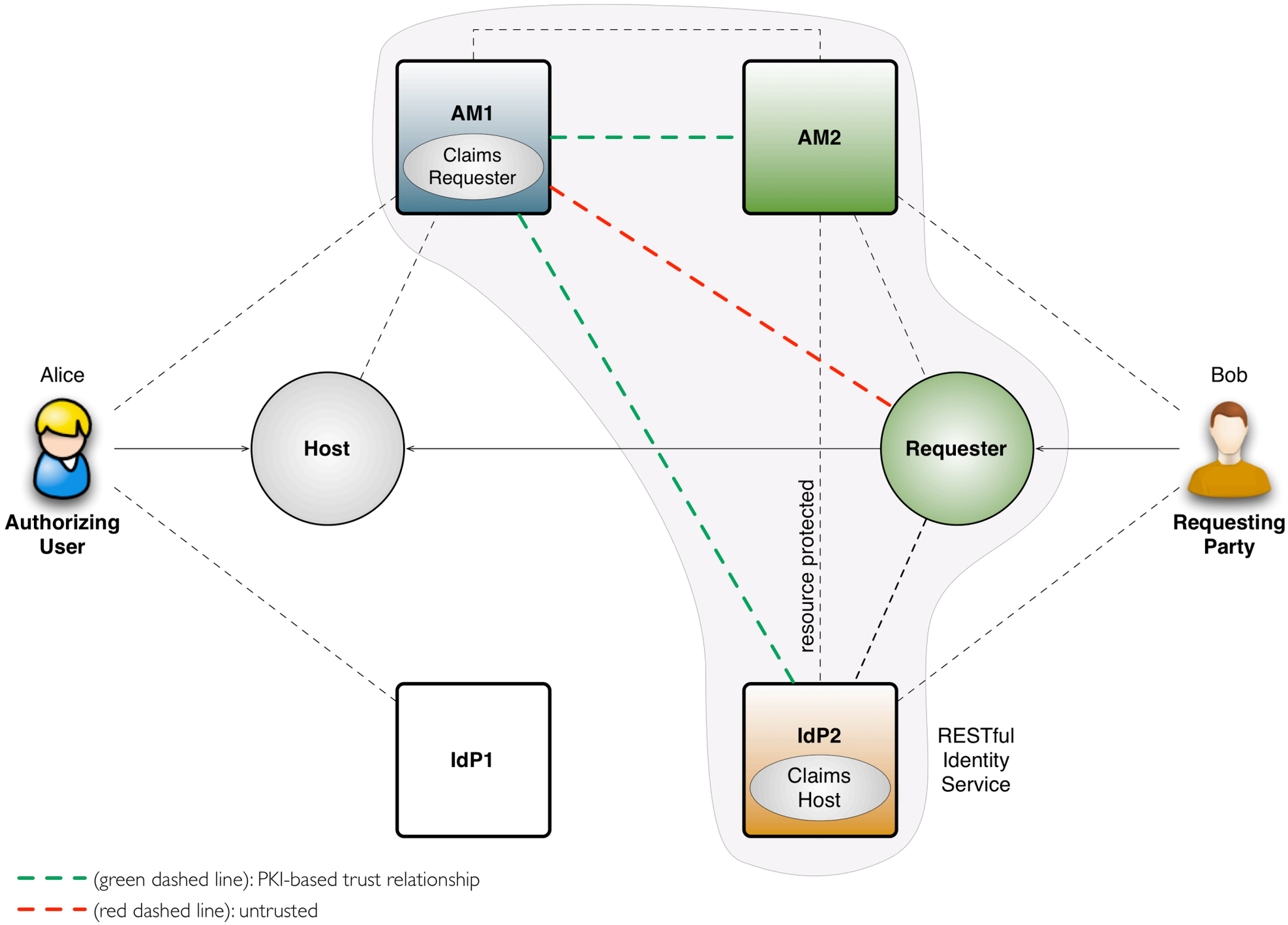
# Step 2 protocol flow



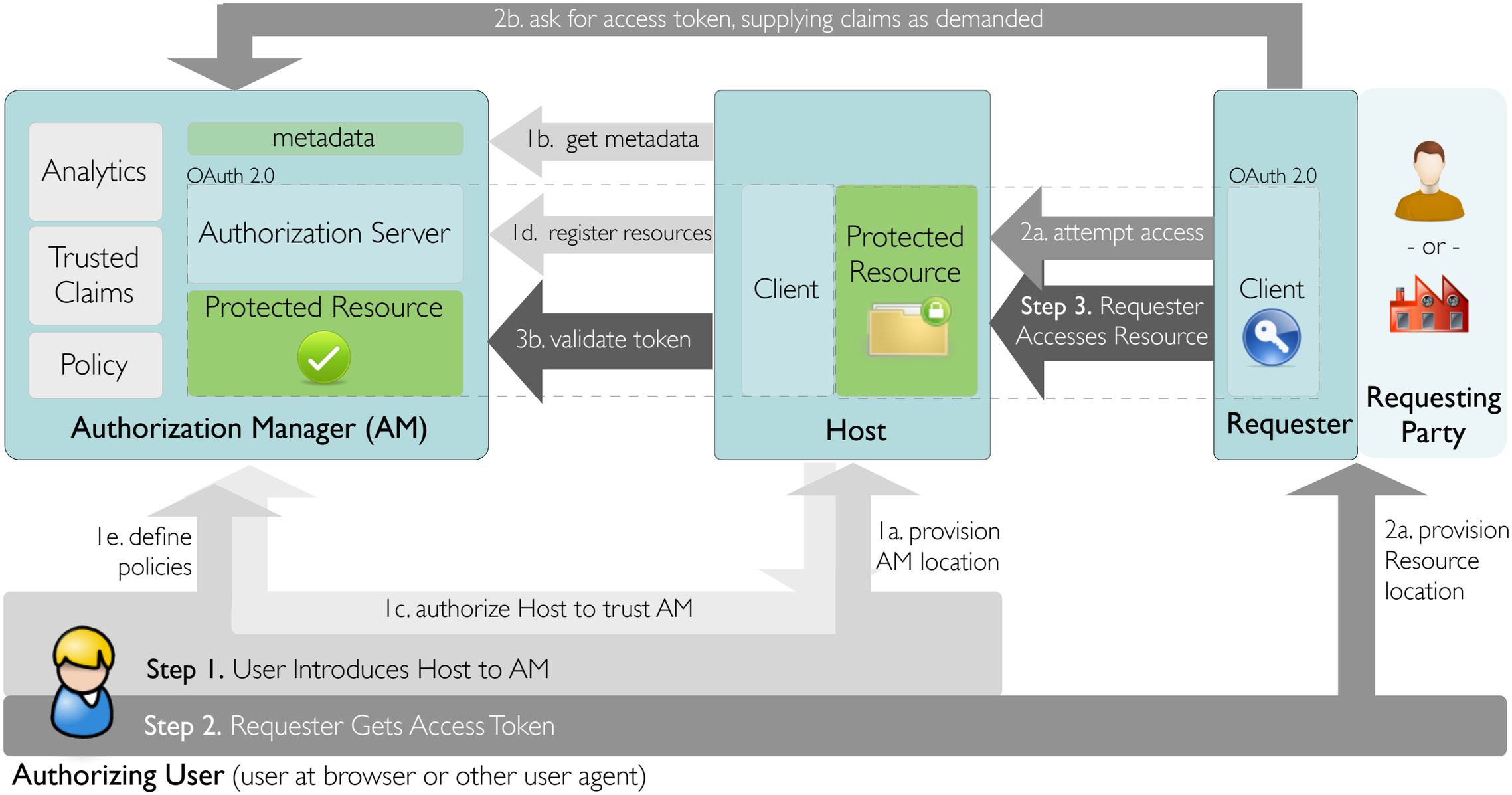
# A possible UX for self-asserted claims about promises



# A potential claims trust model: make them UMA-protected resources

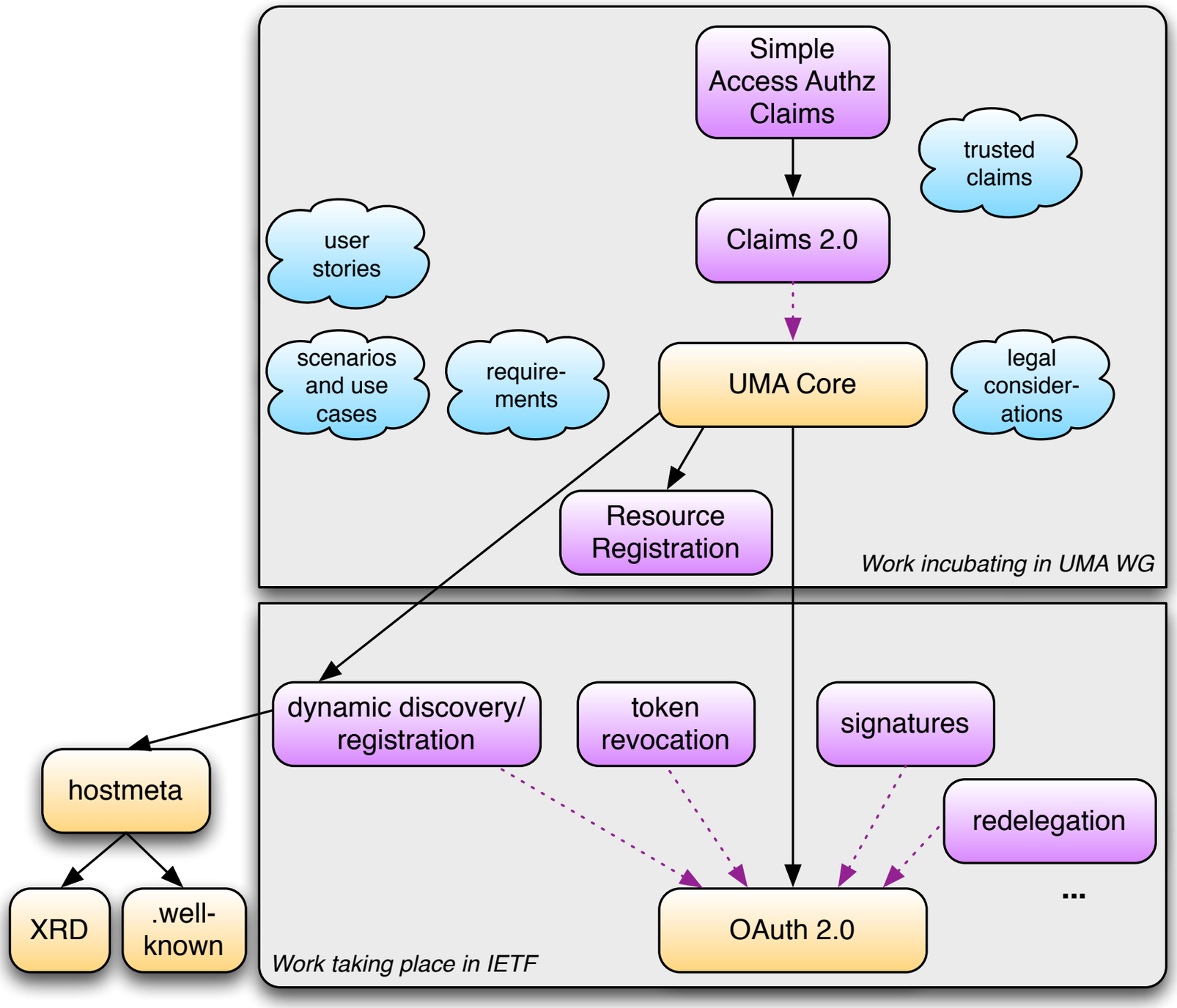


# Step 3 protocol flow



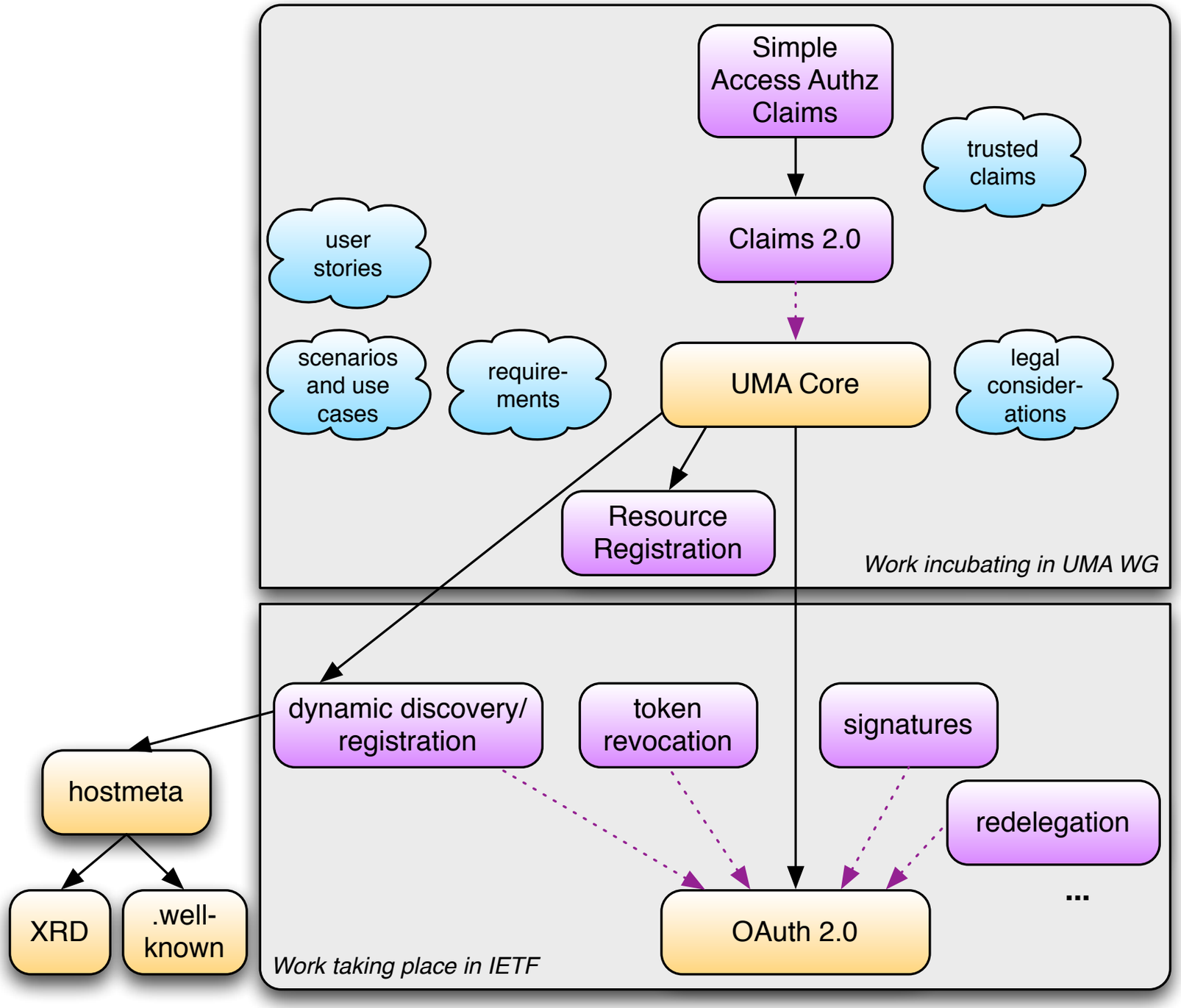
# Status of UMA development

(see also Working Drafts wiki page)



# Status of UMA development

(see also Working Drafts wiki page)




Newcastle University

leeloo

kantara INITIATIVE

**UMA Validator Bounty Program**

Special thanks to Maciej Machulak
and Domenico Catalano for
screenshots and graphics